

A local-global principle for isogenies of prime degree over number fields.

Samuele Anni

March 18, 2013

Abstract

We give a description of the set of exceptional pairs for a number field K , that is the set of pairs $(\ell, j(E))$, where ℓ is a prime and $j(E)$ is the j -invariant of an elliptic curve E over K which admits an ℓ -isogeny locally almost everywhere but not globally. We obtain an upper bound for ℓ in such pairs in terms of the degree and the discriminant of K . Moreover, we prove finiteness results about the number of exceptional pairs.

1 Introduction

Let E be an elliptic curve over a number field K , and let ℓ be a prime number. If we know local information on E , i.e. information over the reduction of E for a set of primes with density one, can we deduce global information about E ?

One of the first to ask this kind of questions was Serge Lang: let E be an elliptic curve over a number field K , and let ℓ be a prime number, if E has non-trivial ℓ -torsion locally at a set of primes with density one, then does E have non-trivial ℓ -torsion over K ? Katz in 1981, see [7], studied this local-global principle: he was able to prove that if E has non-trivial ℓ -torsion locally at a set of primes with density one then there exists a K -isogenous elliptic curve which has non-trivial ℓ -torsion over K . He proved this by reducing the problem to a purely group-theoretic statement. Moreover, he was able to extend the result even further to 2-dimensional abelian varieties and to give a family of counterexamples in dimension 3.

Here we consider the following variation on this question: let E be an elliptic curve over a number field K , and let ℓ be a prime number, if E admits an ℓ -isogeny locally at a set of primes with density one then does E admit an ℓ -isogeny over K ?

Recently, Sutherland has studied this problem, see [17]. Let us recall that, except in the case when the j -invariant is 0 or 1728, whether an elliptic curve admits an ℓ -isogeny over K or not depends only on its j -invariant. As

in [17], we will only consider elliptic curves with j -invariant different from 0 and 1728.

Definition 1.1. *Let K be a number field and E an elliptic curve over K . A pair $(\ell, j(E))$ is said to be exceptional for K if E/K admits an ℓ -isogeny locally almost everywhere but not globally over K .*

For primes of good reduction and not dividing ℓ , the definition of local isogeny is the natural one, and it is recalled in Definition 2.1 below.

Let us remark that if $(\ell, j(E))$ is an exceptional pair for the number field K , then any E_D , quadratic twist of E , gives rise to the same exceptional pair. Indeed, the Galois representation associated to the ℓ -torsion of E and the one of E_D are twist of each other: $\rho_{E_D, \ell} \simeq \chi_D \otimes \rho_{E, \ell}$, where χ_D is a quadratic character. Hence the projective images of such representations are isomorphic.

A curve occurring in an exceptional pair will admit an ℓ -isogeny globally over a small extension of the base field: more precisely, we can state the following Proposition, which is a sharpened version of a result of Sutherland (for a proof see section 3):

Proposition 1.2. *Let E be an elliptic curve defined over a number field K , let ℓ be a prime number and assume $\sqrt{(-1/\ell)} \notin K$. Suppose that E/K admits an ℓ -isogeny locally at a set of primes with density one. Then E admits an ℓ -isogeny over $K(\sqrt{-\ell})$. Moreover, if $\ell = 2, 3$ or $\ell \equiv 1 \pmod{4}$ then E admits a global ℓ -isogeny over K .*

There are examples, for $\ell \equiv 3 \pmod{4}$ and $\ell \geq 7$, in which it is necessary to extend the base field to have a global isogeny. In particular, Sutherland proved that over \mathbb{Q} the following optimal result holds:

Theorem 1.3. (Sutherland, [17, Theorem 2]) *The pair $(7, 2268945/128)$ is the only exceptional pair for \mathbb{Q} .*

This Theorem is proved applying [13, Theorem 1.1], which asserts that for all primes $\ell > 7$, $\ell \equiv 3 \pmod{4}$, the only rational non-cuspidal points on $X_{\text{split}}(\ell)(\mathbb{Q})$ correspond to elliptic curves with complex multiplication (for a definition of this modular curve see section 5). Hence, over \mathbb{Q} there exists only one counterexample to the local-global principle for 7-isogenies and there is none for ℓ -isogenies for $\ell > 7$.

We will prove that a similar dichotomy is true for any number field: the number of counterexamples to the local-global principle about ℓ -isogenies for $\ell > 7$ is always finite and the number of counterexamples to the local-global principle about 7-isogenies and 5-isogenies may or may not be finite, in one case according to the rank of a given elliptic curve, in the other according to a particular condition on the number field.

Namely, the main result of this paper is the following:

Main Theorem. *Let K be a number field of degree d over \mathbb{Q} and discriminant Δ , and let $\ell_K := \max\{\Delta, 6d + 1\}$. The following holds:*

- (1) *if $(\ell, j(E))$ is an exceptional pair for the number field K then $\ell \leq \ell_K$;*
- (2) *if $7 < \ell \leq \ell_K$ then the number of exceptional pairs $(\ell, j(E))$ for K is finite;*
- (3) *if $\ell = 7$ then the number of exceptional pairs for K is finite or infinite, according to the rank of Elkies-Sutherland's elliptic curve:*

$$y^2 = x^3 - 1715x + 33614$$

being zero or positive over K ;

- (4) *if $\ell = 2$ or 3 then there exists no exceptional pair;*
- (5) *if $\ell = 5$, then there exist exceptional pairs if and only if $\sqrt{5}$ belongs to K , in which case the number of exceptional pairs for K is infinite.*

Actually, we prove more precise results that will be discussed in the following sections. Before entering the details of the proofs, let us give a rough idea of our strategy for the point (1) above.

The pair $(\ell, j(E))$ is exceptional for a number field K if and only if the action of $G \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$, the image of the Galois representation associated to the ℓ -torsion of E , on $\mathbb{P}(E[\ell]) \simeq \mathbb{P}^1(\mathbb{F}_\ell)$ has no fixed point, whereas every $g \in G$ leaves a line stable, that is, all $g \in G$ have a reducible characteristic polynomial. Using Dickson's classification of subgroups of $\mathrm{PGL}_2(\mathbb{F}_\ell)$, one sees that, up to conjugation, G has to be either the inverse image of an exceptional group (but this case is known to happen only for small ℓ) or contained in the normalizer of a split Cartan subgroup, that is $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \mid a, b \in \Gamma \right\}$ for Γ a subgroup of \mathbb{F}_ℓ^* .

In the last case, using notations as in [13, section 2] or in section 5 herein, exceptional pairs therefore induce points in $X_{\mathrm{split}}(\ell)(K)$ not lifting to $X_{\mathrm{sp.Car}}(\ell)(K)$ (forgetting cases corresponding to exceptional groups). The existence of such points is in general a wide open question; however, in our case, the reducibility of the characteristic polynomials implies that Γ is actually a subgroup of squares: $\Gamma \subseteq (\mathbb{F}_\ell^*)^2$. By the property of Weil pairing, one deduces that $K(\sqrt{(-1/\ell)}\ell) \subseteq L$, field of definition of the ℓ -isogeny. From this, in the case $\sqrt{(-1/\ell)}\ell \notin K$, we can conclude that the well-known shape of inertia at ℓ inside G gives a contradiction for $\ell > 6[K : \mathbb{Q}] + 1$.

This article is organized as follows. For the convenience of the reader, we recall in section 2 the results obtained by Sutherland in [17, section 2]. In section 3, we study exceptional pairs over arbitrary number fields.

First we deduce the effective version of Sutherland's result, then we describe how to tackle the case not treated by Sutherland and finally we prove the statement (4) of the Main Theorem (see Proposition 3.9). In section 4, we prove, as we already commented, the bound given in (1) of the Main Theorem (Corollary 4.5). In section 5 we discuss finiteness results for the set of exceptional pairs and we prove statements (2) (Theorem 5.3), (5) (Corollary 5.5) and (3) (Proposition 5.6) of the Main Theorem. Finally, in section 6, we give conditions under which an exceptional pair does not have complex multiplication.

2 Sutherland's results

Let us recall the definition of local ℓ -isogeny for an elliptic curve:

Definition 2.1. *Let E be an elliptic curve over a number field K , let ℓ be a prime number. If \mathfrak{p} is a prime of K where E has good reduction, \mathfrak{p} not dividing ℓ , we say that E admits an ℓ -isogeny locally at \mathfrak{p} if the reduction of E modulo \mathfrak{p} admits an ℓ -isogeny defined over the residue field at \mathfrak{p} .*

Let us remark that for a prime \mathfrak{p} of K where E has good reduction, \mathfrak{p} not dividing ℓ , the definition given is equivalent to say that the Néron model of E over the ring of integer of $K_{\mathfrak{p}}$ admits an ℓ -isogeny. This follows essentially because the ℓ -isogeny in this case is étale.

Sutherland has proved, under certain conditions, that for an elliptic curve defined over a number field, the existence of local ℓ -isogenies for a set of primes with density one implies the existence of a global ℓ -isogeny:

Theorem 2.2. (Sutherland [17, Theorem 1]) *Let E be an elliptic curve over a number field K , $j(E) \notin \{0, 1728\}$, and let ℓ be a prime number. Assume that $\sqrt{\left(\frac{-1}{\ell}\right)} \ell \notin K$, and suppose E/K admits an ℓ -isogeny locally at a set of primes with density one.*

Then E admits an ℓ -isogeny over a quadratic extension of K . Moreover, if $\ell \equiv 1 \pmod{4}$ or $\ell < 7$, E admits an ℓ -isogeny defined over K .

Let us recall briefly how this theorem is proved. The main tool used is the theory of Galois representations attached to elliptic curves, see [15], to reduce the problem to a question regarding subgroups of $\mathrm{GL}_2(\mathbb{F}_{\ell})$.

There is a natural action of $\mathrm{GL}_2(\mathbb{F}_{\ell})$ on $\mathbb{P}^1(\mathbb{F}_{\ell})$, and the induced action of $\mathrm{PGL}_2(\mathbb{F}_{\ell})$ is faithful. For an element g of $\mathrm{GL}_2(\mathbb{F}_{\ell})$ or of $\mathrm{PGL}_2(\mathbb{F}_{\ell})$, we will denote, respectively, by $\mathbb{P}^1(\mathbb{F}_{\ell})/g$ the set of g -orbits of $\mathbb{P}^1(\mathbb{F}_{\ell})$ and by $\mathbb{P}^1(\mathbb{F}_{\ell})^g$ the set of elements fixed by g .

Lemma 2.3. (Sutherland [17, Lemma 1]) *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_{\ell})$ whose image H in $\mathrm{PGL}_2(\mathbb{F}_{\ell})$ is not contained in $\mathrm{SL}_2(\mathbb{F}_{\ell})/\{\pm 1\}$. Suppose $|\mathbb{P}^1(\mathbb{F}_{\ell})^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_{\ell})^G| = 0$.*

Then $\ell \equiv 3 \pmod{4}$ and the following holds:

- (1) H is dihedral of order $2n$, where $n > 1$ is an odd divisor of $(\ell-1)/2$;
- (2) G is properly contained in the normalizer of a split Cartan subgroup;
- (3) $\mathbb{P}^1(\mathbb{F}_\ell)/G$, the set of G -orbits of $\mathbb{P}^1(\mathbb{F}_\ell)$, contains an orbit of size 2.

This result is an application of the orbit-counting lemma combined with Dickson's classification of subgroups of $\mathrm{PGL}_2(\mathbb{F}_\ell)$, see [5] or [10], and it is one of the key steps in the proof of Theorem 2.2. Let us notice that if the hypotheses of Lemma 2.3 are satisfied, then it follows that $\ell \neq 3$ because $n > 1$ in (1).

Remark 2.4. Given an elliptic curve E over a number field K , the compatibility between $\rho_{E,\ell}$, the Galois representation associated to the ℓ -torsion group $E[\ell]$, and the Weil pairing on $E[\ell]$ implies that for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ we have $\sigma(\zeta_\ell) = \zeta_\ell^{\det(\rho_{E,\ell}(\sigma))}$, where ζ_ℓ is an ℓ -root of unity. Hence, ζ_ℓ is in K if and only if $G = \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$ is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)$. Moreover, using the Gauss sum: $\sum_{n=0}^{\ell-1} \zeta_\ell^{n^2} = \sqrt{(-1/\ell)} \ell$ and denoting by H the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$, it follows that H is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$ if and only if $\sqrt{(-1/\ell)} \ell$ is in K .

Sketch of the proof of Theorem 2.2. For every $g \in G = \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$, it follows from Chebotarev density theorem that we can choose $\mathfrak{p} \subset \mathcal{O}_K$ so that $g = \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ and E admits an ℓ -isogeny locally at \mathfrak{p} . The Frobenius endomorphism fixes a line in $E[\ell]$, hence $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$.

If $|\mathbb{P}^1(\mathbb{F}_\ell)^G| > 0$, then $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ fixes a linear subspace of $E[\ell]$ which is the kernel of an ℓ -isogeny defined over K .

Hence, let us assume $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$. No subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ satisfies $|\mathbb{P}^1(\mathbb{F}_2)^G| = 0$ and $|\mathbb{P}^1(\mathbb{F}_2)^g| > 0$ for all $g \in G$, so $\ell \neq 2$. The hypotheses on K combined with the Weil pairing on the ℓ -torsion implies that some element of G has a non-square determinant, hence the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ does not lie in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. The hypotheses of Lemma 2.3 are satisfied, thus $\ell \equiv 3 \pmod{4}$, $\ell \neq 3$, and $\mathbb{P}^1(\mathbb{F}_\ell)/G$ contains an orbit of size 2. Let $x \in \mathbb{P}^1(\mathbb{F}_\ell)$ be an element of this orbit, its stabilizer is a subgroup of index 2. By Galois theory, it corresponds to a quadratic extension of K over which E admits an isogeny of degree ℓ (actually, two such isogenies). \square

3 Exceptional pairs and Galois representations

The study of the local-global principle about ℓ -isogenies over an arbitrary number field K depends on $\sqrt{\left(\frac{-1}{\ell}\right)}\ell$ belonging to K or not.

First, let us assume that $\sqrt{\left(\frac{-1}{\ell}\right)}\ell$ does not belong to K . Theorem 2.2 implies that an exceptional pair for K , a number field not containing $\sqrt{\left(\frac{-1}{\ell}\right)}\ell$, is no longer exceptional for a quadratic extension of K : in this section we will describe this extension.

Proposition 3.1. *Let $(\ell, j(E))$ be an exceptional pair for the number field K , $j(E) \notin \{0, 1728\}$, and assume that $\sqrt{\left(\frac{-1}{\ell}\right)}\ell \notin K$. Let G be $\rho_{E,\ell}(\text{Gal}(\overline{\mathbb{Q}}/K))$ and let H be its image in $\text{PGL}_2(\mathbb{F}_\ell)$. Let $\mathcal{C} \subset G$ be the preimage of the maximal cyclic subgroup of H . Then $\det(\mathcal{C}) \subseteq (\mathbb{F}_\ell^*)^2$, where $(\mathbb{F}_\ell^*)^2$ denotes the group of squares in \mathbb{F}_ℓ^* .*

Proof. Let $(\ell, j(E))$ be an exceptional pair for the number field K , and assume that $\sqrt{\left(\frac{-1}{\ell}\right)}\ell \notin K$. By Remark 2.4, this implies that H is not contained in $\text{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$ hence, applying Lemma 2.3, we have that $\ell \equiv 3 \pmod{4}$, H is dihedral of order $2n$, where $n > 1$ is an odd divisor of $(\ell-1)/2$ and G is properly contained in the normalizer of a split Cartan subgroup. In particular $(n, \ell+1) = 1$ and $(n, \ell) = 1$, because n is odd and it is a divisor of $\ell-1$.

Let $A \in G \subset \text{GL}_2(\mathbb{F}_\ell)$ be a preimage of some generator of the maximal cyclic subgroup inside H . Let us prove that A is conjugate in $\text{GL}_2(\mathbb{F}_\ell)$ to a matrix of the type $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$, with $\alpha, \beta \in \mathbb{F}_\ell^*$ and α/β of order n in \mathbb{F}_ℓ^* .

Extending the scalars to \mathbb{F}_{ℓ^2} if necessary, we can put A in its Jordan normal form. Then either $A \cong \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ with $\alpha, \beta \in \mathbb{F}_{\ell^2}$, or $A \cong \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$. Since we have $A^n = \lambda \cdot \text{Id}$, for $\lambda \in \mathbb{F}_\ell^*$, and $(n, \ell) = 1$ then the second case cannot occur. We claim that $\alpha, \beta \in \mathbb{F}_\ell^*$. In fact, let us proceed by contradiction: if $\alpha, \beta \in \mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$ then $\beta = \overline{\alpha}$, the conjugate of α over \mathbb{F}_ℓ . This means that $\mathbb{P}^1(\mathbb{F}_\ell)^A$ is empty because A has no eigenvalues in \mathbb{F}_ℓ and this is not possible because E admits an ℓ -isogeny locally everywhere and by Chebotarev density theorem $A = \rho_{E,\ell}(\text{Frob}_{\mathfrak{p}})$ with $\mathfrak{p} \subset \mathcal{O}_K$ prime. Hence $\alpha, \beta \in \mathbb{F}_\ell^*$.

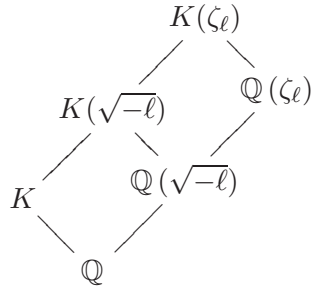
Let us write $\alpha = \mu^i$ and $\beta = \mu^j$ for some generator μ of \mathbb{F}_ℓ^* . Then $\mu^{in} = \alpha^n = \beta^n = \mu^{jn}$ so that $\mu^{n(i-j)} = 1$ and $n(j-i) \equiv 0 \pmod{\ell-1}$. As n is odd, $(j-i)$ has to be even, hence so is $(i+j)$. From this it follows that $\det(A) = \alpha\beta = \mu^{i+j}$ is a square in \mathbb{F}_ℓ^* . Moreover, since A is a preimage of some generator of the maximal cyclic subgroup inside H , then α/β must have order n . \square

Remark 3.2. Let $(\ell, j(E))$ be an exceptional pair for the number field K , $j(E) \notin \{0, 1728\}$ and $\sqrt{\left(\frac{-1}{\ell}\right)} \ell \notin K$. Since the projective image of the Galois representation associated to E is dihedral of order $2n$, with n odd divisor of $(\ell-1)/2$, the order of G , image of the Galois representation, satisfies:

$$|G| \mid ((\ell-1) \cdot 2n) \mid \left((\ell-1) \cdot \frac{(\ell-1)}{2} \cdot 2 \right) = (\ell-1)^2.$$

Proposition 3.3. *Let $(\ell, j(E))$ be an exceptional pair for the number field K , $j(E) \notin \{0, 1728\}$, and assume that $\sqrt{\left(\frac{-1}{\ell}\right)} \ell$ does not belong to K . Then E admits an ℓ -isogeny over $K(\sqrt{-\ell})$ (and actually, two such isogenies).*

Proof. We can apply Theorem 2.2, and we have that $\ell \equiv 3 \pmod{4}$ and $\ell \geq 7$ since $(\ell, j(E))$ is an exceptional pair. Since $\sqrt{-\ell} \notin K$, then also ζ_ℓ , the ℓ -th root of unity, is not in K by ramification theory.



Since $\ell \equiv 3 \pmod{4}$, the quadratic subfield of $\mathbb{Q}(\zeta_\ell)$ is $\mathbb{Q}(\sqrt{-\ell})$. In particular, $\text{Gal}(K(\zeta_\ell)/K(\sqrt{-\ell})) \subseteq (\mathbb{F}_\ell^*)^2$, the subgroup of squares inside \mathbb{F}_ℓ^* . If ℓ does not divide the discriminant of K then the previous inclusion is an equality, since the ramifications are disjoint. Let, as before, $\rho_{E,\ell}: \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GL}_2(\mathbb{F}_\ell)$ be the Galois representation associated to E and let G be its image.

It follows, using notation of Proposition 3.1, that E admits one isogeny (actually two) on the quadratic extension L/K corresponding to the Cartan subgroup \mathcal{C} which is the subgroup of diagonal matrices inside G . By Proposition 3.1, the elements of \mathcal{C} have square determinants.

On the other hand, from the properties of the Weil pairing on the ℓ -torsion, for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/K)$ we have that $\det(\rho_{E,\ell}(\sigma)) = \chi_\ell(\sigma)$, where χ_ℓ is the mod ℓ cyclotomic character. Hence, \mathcal{C} is the kernel of the character $\varphi: G \rightarrow \mathbb{F}_\ell^*/(\mathbb{F}_\ell^*)^2 \cong \{\pm 1\}$ which makes the following diagram commute:

$$\begin{array}{ccccc}
 \text{Gal}(\overline{\mathbb{Q}}/K) & \xrightarrow{\rho_{E,\ell}} & G & \xrightarrow{\varphi} & \mathbb{F}_\ell^*/(\mathbb{F}_\ell^*)^2 \cong \{\pm 1\} \\
 & & \downarrow \det & \searrow \chi_\ell & \nearrow \\
 & & \text{Gal}(K(\zeta_\ell)/K) & \hookrightarrow & \mathbb{F}_\ell^* \cong \text{Aut}(\mu_\ell)
 \end{array}$$

The character of $\text{Gal}(\overline{\mathbb{Q}}/K)$ induced by φ is not trivial because there is an element in G with non square determinant since $\sqrt{-\ell}$ is not in K . By

Galois theory, the kernel of φ corresponds to a quadratic extension of K , which contains $\sqrt{-\ell}$ by construction. This implies that the extension over which E admits a global ℓ -isogeny is $K(\sqrt{-\ell})$. \square

Combining Proposition 3.3 and Theorem 2.2, we have proved the following result (which is Proposition 1.2 of the Introduction):

Proposition 3.4. *Let E be an elliptic curve defined over a number field K , $j(E) \notin \{0, 1728\}$. Let ℓ be a prime number and let $\sqrt{\left(\frac{-1}{\ell}\right)\ell} \notin K$. Suppose that E/K admits an ℓ -isogeny locally at a set of primes with density one, then E admits an ℓ -isogeny over $K(\sqrt{-\ell})$. Moreover, if $\ell = 2, 3$ or $\ell \equiv 1 \pmod{4}$ then E admits a global ℓ -isogeny over K .*

Now let us assume that $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ belongs to K .

We want to consider the case of subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$ which do not fix any point of $\mathbb{P}^1(\mathbb{F}_\ell)$ but whose elements do fix points. The following Lemma is a variation on the result, due to Sutherland, that we stated in the present article as Lemma 2.3, see [17, Lemma 1 and Proposition 2]. This Lemma will be the key in understanding the case in which $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ belongs to K . We will denote by S_n (resp. A_n) the symmetric (resp. alternating) group on n -elements.

Lemma 3.5. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ whose image H in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. Suppose $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$. Then $\ell \equiv 1 \pmod{4}$ and one of the followings holds:*

- (1) H is dihedral of order $2n$, where $n \in \mathbb{Z}_{>1}$ is a divisor of $\ell-1$;
- (2) H is isomorphic to one of the following exceptional groups: A_4 , S_4 or A_5 .

Proof. No subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ satisfies the hypotheses of the lemma, so we assume $\ell > 2$. The orbit-counting lemma yields:

$$|\mathbb{P}^1(\mathbb{F}_\ell)/H| = \frac{1}{|H|} \sum_{h \in H} |\mathbb{P}^1(\mathbb{F}_\ell)^h| \geq \frac{1}{|H|}(\ell + |H|) > 1$$

since $|\mathbb{P}^1(\mathbb{F}_\ell)^h| > 0$ for all $h \in H$ and $|\mathbb{P}^1(\mathbb{F}_\ell)^h| = (\ell+1)$ when h is the identity. If ℓ divides $|H|$ then H contains an element h of order ℓ and $\mathbb{P}^1(\mathbb{F}_\ell)/h$ consists of two orbits, of sizes 1 and ℓ , therefore a fortiori $(1 <) |\mathbb{P}^1(\mathbb{F}_\ell)/H| \leq 2$. But this contradicts the assumption $|\mathbb{P}^1(\mathbb{F}_\ell)^H| = 0$. Hence $\ell \nmid |H|$.

By Dickson's classification of subgroups of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ it follows that H can be either cyclic, or dihedral or isomorphic to one the following groups: S_4 , A_4 , A_5 . We can exclude that H is cyclic. Let us indeed assume otherwise, and write $H = \langle h \rangle$. This implies that $\mathbb{P}^1(\mathbb{F}_\ell)^h = \mathbb{P}^1(\mathbb{F}_\ell)^H$ and since

$|\mathbb{P}^1(\mathbb{F}_\ell)^h| > 0$ by hypothesis, we have a contradiction with $|\mathbb{P}^1(\mathbb{F}_\ell)^H| = 0$. Hence H is either dihedral, or isomorphic to S_4 , or to A_4 , or to A_5 .

By [17, Proposition 2], since H is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$, the size of the set of h -orbits of $\mathbb{P}^1(\mathbb{F}_\ell)$ is even for each $h \in H$. Moreover, as $|\mathbb{P}^1(\mathbb{F}_\ell)^h| > 1$, all h are diagonalizable on \mathbb{F}_ℓ . Then, applying the orbit-counting lemma, we have

$$\begin{aligned} |\mathbb{P}^1(\mathbb{F}_\ell)/h| &= \frac{1}{\mathrm{ord}(h)} \sum_{h' \in \langle h \rangle} |\mathbb{P}^1(\mathbb{F}_\ell)^{h'}| = \\ &= \frac{1}{\mathrm{ord}(h)} ((\mathrm{ord}(h)-1)2 + \ell + 1) = 2 + \frac{\ell-1}{\mathrm{ord}(h)} \end{aligned} \quad (1)$$

where $\langle h \rangle$ denotes the cyclic subgroup of H generated by h . In particular, for elements of order 2 this implies that $\ell \equiv 1 \pmod{4}$.

Let us suppose that H is a dihedral group of order $2n$. Then there exists $h \in H$ of order n , so equation (1) implies that n divides $\ell-1$. \square

Note that, in the course of the above proof, we have shown the following:

Corollary 3.6. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ whose image H in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. Suppose $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$. If H is dihedral of order $2n$, where $n \in \mathbb{Z}_{>1}$ is a divisor of $\ell-1$, then G is properly contained in the normalizer of a split Cartan subgroup and $\mathbb{P}^1(\mathbb{F}_\ell)/G$ contains an orbit of size 2.*

Corollary 3.7. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ whose image H in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. Suppose $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$. Then:*

- if H is isomorphic to A_4 then $\ell \equiv 1 \pmod{12}$;
- if H is isomorphic to S_4 then $\ell \equiv 1 \pmod{24}$;
- if H is isomorphic to A_5 then $\ell \equiv 1 \pmod{60}$.

Proof. This is an application of the orbit-counting lemma. In A_4 there are elements of order 2 and 3, and we have $\ell > 3$ since $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$. The equation (1) for elements of order 3 implies that $\ell-1$ is divisible by 3, so, since $\ell \equiv 1 \pmod{4}$, then $\ell \equiv 1 \pmod{12}$.

Applying [17, Proposition 2], we see that the parity of the values of equation (1) determines the sign as permutation of any element of $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Since H is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$, the value of equation (1) has to be even for every $h \in H$. If H is isomorphic to S_4 , then it contains elements of order 4 and this implies that $\ell-1$ is divisible by 8. Repeating the argument for elements of order 3 we conclude that $\ell \equiv 1 \pmod{24}$.

Analogously, if H is isomorphic to A_5 then $\ell > 5$: not all matrices in $\mathrm{PSL}_2(\mathbb{F}_5) \simeq A_5$ leave a line stable. Since there are elements of order 3 and 5, then $\ell-1$ is divisible by 3 and 5. So, since $\ell \equiv 1 \pmod{4}$, we have $\ell \equiv 1 \pmod{60}$. \square

Proposition 3.8. *Let E be an elliptic curve over a number field K of degree d over \mathbb{Q} , $j(E) \notin \{0, 1728\}$, and let ℓ be a prime number. Let us suppose $\sqrt{(-1/\ell)} \ell \in K$ and that E/K admits an ℓ -isogeny locally at a set of primes with density one. Then:*

- (1) *if $\ell \equiv 3 \pmod{4}$ the elliptic curve E admits a global ℓ -isogeny over K ;*
- (2) *if $\ell \equiv 1 \pmod{4}$ the elliptic curve E admits an ℓ -isogeny over a finite extension of K , which can ramify only at primes dividing the conductor of E and ℓ . Moreover, if $\ell \equiv -1 \pmod{3}$ or if $\ell \geq 60d+1$, then E admits an ℓ -isogeny over a quadratic extension of K .*

Proof. Since $\sqrt{(-1/\ell)} \ell$ is contained in K , the projective image H of the Galois representation $\rho_{E,\ell}$ is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$, as discussed in Remark 2.4, so we can apply Lemma 3.5. This means that if the pair $(\ell, j(E))$ is an exceptional pair then $\ell \equiv 1 \pmod{4}$ and H has to be either a dihedral group of order $2n$, with n dividing $\ell-1$, or an exceptional subgroup.

If the elliptic curve E admits an ℓ -isogeny over a number field L/K then there exists a one dimensional $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ -stable subspace of $E[\ell]$. This subspace corresponds to a subgroup of the image of the Galois representation. In particular, the extension L of K over which the isogeny is defined can only ramify at primes where the representation is ramified, that is, only at primes of K dividing the conductor of E or ℓ .

If $\ell \geq 60d+1$ then H cannot be isomorphic to A_4 , or to S_4 or A_5 , for a proof of this fact see [11, p. 36]. Analogously, by Corollary 3.7, exceptional images cannot occur if $\ell \equiv -1 \pmod{3}$. Hence, by Corollary 3.6, in these cases the image of the Galois representation associated to E is conjugated to the normalizer of a Cartan subgroup which contains the Cartan subgroup itself with index 2. By Galois theory, then E admits a global isogeny over a quadratic extension of K . \square

Let us now describe all the possibilities that can occur at 2, 3 and 5:

Proposition 3.9. *Given a number field K , if $\ell = 2, 3$ then there exists no exceptional pair. If $\ell = 5$, then there exist exceptional pairs $(5, j(E))$ only if $\sqrt{5}$ belongs to K . Moreover, $\mathbb{P}\rho_{E,5}(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$ is a dihedral group of order dividing 8.*

Proof. As remarked in the proof of Theorem 2.2, for $\ell=2$ there exists no exception to the local-global principle. Take $\ell=3$. If $\sqrt{-3}$ is not in K then

there exists no exceptional pair since, by Lemma 2.3, the projective image is a dihedral group of order $2n$ with $n \in \mathbb{Z}_{>1}$ odd (dividing $3-1$). Similarly if $\sqrt{-3}$ belongs to K there exists no exceptional pair since, by Lemma 3.5, $\ell \equiv 1 \pmod{4}$. For $\ell=5$ we have that if $\sqrt{5}$ is not in K then there exists no exceptional pair by Lemma 2.3. Moreover, if $\sqrt{5}$ is in K then by Lemma 3.5 combined with Corollary 3.7, the projective image can only be a dihedral group of order dividing 8. \square

4 Bounds

In this section we prove statement (1) of the Main Theorem.

4.1 Image of the inertia

Let M be a complete field with respect to a discrete valuation v , which is normalized, i.e. $v(M^*) = \mathbb{Z}$. Let \mathcal{O}_M be its ring of integers, λ the maximal ideal of \mathcal{O}_M and $k = \mathcal{O}_M/\lambda$ the residue field. We suppose M of characteristic 0, k finite of characteristic $\ell > 0$ and $e = v(\ell) < \infty$. Let E be an elliptic curve having semi-stable reduction over M and let \mathcal{E} be its Néron model over \mathcal{O}_M . Since M is of characteristic 0, we know that $E[\ell](\overline{M})$ is an \mathbb{F}_ℓ -vector space of dimension 2. Let $\overline{\mathcal{E}}$ be the reduction of \mathcal{E} modulo λ , then $\overline{\mathcal{E}}$ is a group scheme defined over k whose ℓ -torsion is an \mathbb{F}_ℓ -vector space with dimension strictly lower than 2. Hence, the kernel of the reduction map, can be either isomorphic to \mathbb{F}_ℓ (ordinary case) or to the whole $E[\ell]$ (supersingular case).

Serre, in [15, Proposition 11, Proposition 12 and page 272], described all possible shapes of the image of \mathcal{I}_ℓ , the inertia subgroup at ℓ , for the supersingular case and for the ordinary case:

Proposition 4.1. (*Serre, supersingular case*) *Let E be an elliptic curve over M and let $e = v(\ell) \geq 1$. Suppose that E has good supersingular reduction at ℓ . Then the image of \mathcal{I}_ℓ through the Galois representation associated to E , $\rho_{E,\ell} : \text{Gal}(\overline{M}/M) \rightarrow \text{GL}_2(\mathbb{F}_\ell)$, is cyclic of order either $(\ell^2-1)/e$ or $\ell(\ell-1)/e$.*

The two cases depend on the action of the tame inertia.

If the tame inertia acts via powers of the fundamental character of level 2, and not 1, it follows that the Newton polygon, with respect to the elliptic curve, is not broken, and that the tame inertia is given by the e -power of the fundamental character of level 2. Hence it has a cyclic image of order $(\ell^2-1)/e$.

If the elliptic curve considered is supersingular, but the tame inertia acts via powers of the fundamental character of level 1, it follows that the relevant Newton polygon is broken, and there are points in the ℓ -torsion of the corresponding formal group which have valuation with denominator divisible by ℓ

(this follows from [15, page 272]). So the image of inertia has order $\ell(\ell-1)/e$.

We will now describe the ordinary case:

Proposition 4.2. (*Serre, ordinary case*) *Let E be an elliptic curve over M and let $e = v(\ell) \geq 1$. Suppose that E has semistable ordinary reduction at ℓ . Then the image of \mathcal{I}_ℓ through the Galois representation associated to E , $\rho_{E,\ell} : \text{Gal}(\overline{M}/M) \rightarrow \text{GL}_2(\mathbb{F}_\ell)$, is cyclic of order either $(\ell-1)/e$ or $\ell(\ell-1)/e$, and it can be represented, after the choice of an appropriate basis, respectively as $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} * & \star \\ 0 & 1 \end{pmatrix}$ with $*$ $\in \mathbb{F}_\ell^*$ and $\star \in \mathbb{F}_\ell$.*

4.2 Computation of the bound

Let E_λ be an elliptic curve defined over a complete field M with maximal ideal λ , let

$$d' = \begin{cases} 1 & \text{if } j(E) \not\equiv 0, 1728 \pmod{\lambda}, \\ 2 & \text{if } j(E) \equiv 1728 \pmod{\lambda}, \ell \geq 5 \\ 3 & \text{if } j(E) \equiv 0 \pmod{\lambda}, \ell \geq 5, \\ 6 & \text{if } j(E) \equiv 0 \pmod{\lambda}, \ell = 3, \\ 12 & \text{if } j(E) \equiv 0 \pmod{\lambda}, \ell = 2. \end{cases} \quad (2)$$

Then E_λ , or a quadratic twist, has semistable reduction over a finite extension of M with degree d' , see for instance [1, pp. 33-52] or [9, Proposition 1 and Théorème 1].

We can now give the main result of this article:

Theorem 4.3. *Let $(\ell, j(E))$ be an exceptional pair for the number field K of degree d over \mathbb{Q} , such that $\sqrt{(-1/\ell)} \ell \notin K$, $j(E) \notin \{0, 1728\}$. Then $\ell \equiv 3 \pmod{4}$ and $7 \leq \ell \leq 6d+1$.*

Proof. Since the pair $(\ell, j(E))$ is exceptional, E admits an ℓ -isogeny locally at a set of primes with density one and Proposition 3.4 states that it admits an ℓ -isogeny over $L = K(\sqrt{-\ell})$ and $\ell \equiv 3 \pmod{4}$.

Let us consider the completion K_λ of K at λ , a prime above ℓ , and let M be the smallest extension of K_λ over which $E_\lambda := E \otimes K_\lambda$ gets semistable reduction. After replacing E by a quadratic twist if necessary, we can assume that the extension M/K_λ has degree less or equal to 3, according to (2), since $\ell \geq 7$. Let \overline{E} be the reduction of $E_{\lambda'} := E \otimes M$ modulo λ' , for λ' the prime above λ .

We consider the inertia subgroup of the image of the Galois representation associated to E .

Assume that the reduction \overline{E} is supersingular. The inertia has image isomorphic to a cyclic group of order $(\ell^2-1)/m$ or $\ell(\ell-1)/m$, where m is less or equal to $3d$, according to the degree of the extension needed to have semistable reduction. On the other hand, the Galois representation has image

of order dividing $(\ell-1)^2$ by Remark 3.2. The second case leads directly to a contradiction. In the first case, the inertia, that is isomorphic to a non-split torus in $\mathrm{GL}_2(\mathbb{F}_\ell)$, is a subgroup of the image of the Galois representation, that is contained in the normalizer of a split Cartan, as stated in Lemma 2.3. Hence, this is impossible unless

$$(\ell^2-1)/m \mid (\ell-1)^2.$$

This means that $(\ell+1)/m \mid (\ell-1)$, so that $(\ell+1)/m \mid 2$, hence $\ell \leq 2m-1$. The pair $(\ell, j(E))$ is exceptional, so $\ell \equiv 3 \pmod{4}$ and $\ell \geq 7$, hence we have the following bound: $\ell \equiv 3 \pmod{4}$ and $7 \leq \ell \leq 2m-1 \leq 6d-1$.

We have proved that if $\ell > 2m-1$, \overline{E} is not supersingular, so it is ordinary (E_λ is semistable over M). By Proposition 3.3, the elliptic curve E admits two ℓ -isogenies over $L = K(\sqrt{-\ell})$, which are conjugate over L . By Lemma 2.3, the image G of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acting on $E[\ell](\overline{K})$ is a subgroup of the normalizer N of a split Cartan subgroup C . From Proposition 3.3, we know that $N/C \simeq \mathrm{Gal}(L/K) \neq \{1\}$, so the image of an inertia subgroup \mathcal{I}_λ at the place λ of K is a subgroup of G whose image in N/C is non-trivial. On the other hand, Proposition 4.2 shows that, if $(\ell-1)/m > 2$, then \mathcal{I}_λ contains a cyclic subgroup of order larger or equal to 3 (for another argument see [12, p. 118]). It follows that \mathcal{I}_λ contains a non-trivial Cartan subgroup (of shape $\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \Gamma \right\}$ for a certain non trivial subgroup Γ of \mathbb{F}_ℓ), even after restriction of the scalars to $\mathrm{Gal}(\overline{M}/M)$. This is a contradiction with Proposition 4.2, as the latter says that the restriction of \mathcal{I}_λ to $\mathrm{Gal}(\overline{M}/M)$ is a semi-Cartan subgroup (or a Borel). Hence, $(\ell-1)/m \leq 2$ so we have $\ell \equiv 3 \pmod{4}$ and $7 \leq \ell \leq 2m+1 \leq 6d+1$. \square

Remark 4.4. It is clear that Theorem 4.3 implies the result obtained by Sutherland in the case $K = \mathbb{Q}$.

The previous Theorem, combined with Remark 2.4, implies point (1) of the Introduction's Main Theorem, namely:

Corollary 4.5. *Let $(\ell, j(E))$ be an exceptional pair for the number field K of degree d over \mathbb{Q} and discriminant Δ , $j(E) \notin \{0, 1728\}$, and let $\ell_K := \max\{\Delta, 6d+1\}$. Then $\ell \leq \ell_K$.*

Proof. If $(\ell, j(E))$ is an exceptional pair for the number field K then we distinguish two cases according to the projective image being contained or not in $\mathrm{SL}_2(\mathbb{F}_\ell)/\pm 1$. This corresponds to a condition about $\sqrt{(-1/\ell)}\ell$ belonging to K or not. If $\sqrt{(-1/\ell)}\ell \notin K$ we can apply Theorem 4.3 and conclude that $7 \leq \ell \leq 6d+1$. While, if $\sqrt{(-1/\ell)}\ell \in K$, then $\ell \mid \Delta$. \square

5 Finiteness of the exceptional pairs

Given a number field K of degree d over \mathbb{Q} and discriminant Δ , the local-global principles for ℓ -isogenies holds whenever $\ell > \ell_k := \max\{\Delta, 6d+1\}$ or $\ell = 2, 3$ by Corollary 4.5 and Proposition 3.9. In this section we analyze what happens for primes smaller than the bound obtained. In particular we will prove that the local-global principle about ℓ -isogenies for elliptic curves over number fields admits only a finite number of exceptions if $\ell > 7$. We will also study the behaviour of the local-global principle at 5 and 7.

Let K be a number field and let C/K be a projective smooth curve defined over K and genus g . Our arguments will rely on the classical trichotomy between curves of genus 0, 1 and higher. When the genus is 0, the curve is isomorphic to \mathbb{P}_K^1 over an algebraic closure of K and therefore $C(K)$, the set of K -rational points, is either empty or infinite. If the genus of C is 1 and $C(K)$ contains at least one point over K then C/K is an elliptic curve over K and the Mordell-Weil theorem shows that $C(K)$ is a finitely generated abelian group: $C(K) \cong T \oplus \mathbb{Z}^r$, where T is the torsion subgroup and r is a non-negative integer called the rank of the elliptic curve, whereas if $g \geq 2$, Faltings Theorem states that the set of K -rational points is finite.

In this section we will recall some theory of modular curves.

Let $\ell \geq 5$ be a prime number and let $\mathbb{Z}[\zeta_\ell]$ be the subring of \mathbb{C} generated by a root of unity of order ℓ . The modular curve $X(\ell)$ is the compactified fine moduli space which classify pairs (E, α) , where E is a generalized elliptic curve over a scheme S over $\text{Spec}(\mathbb{Z}[1/\ell, \zeta_\ell])$ and $\alpha : (\mathbb{Z}/\ell\mathbb{Z})_S^2 \xrightarrow{\sim} E[\ell]$ is an isomorphism of group schemes over S which is a full level ℓ -structure, up to isomorphism of pairs i.e. isomorphisms of elliptic curves which preserve the level structure. A full level ℓ -structure on a generalized elliptic curve E over S is a pair of points (P_1, P_2) , satisfying $P_1, P_2 \in E[\ell]$ and $e_\ell(P_1, P_2) = \zeta_\ell$ where e_ℓ is the Weil pairing on $E[\ell]$. Let us recall that a full level ℓ -structure corresponds to give a symplectic pairing on $(\mathbb{Z}/\ell\mathbb{Z})^2$ via $\langle (1, 0), (0, 1) \rangle = \zeta_\ell$. For more details, see [8] or [6].

Let G be a subgroup of $GL_2(\mathbb{Z}/\ell\mathbb{Z})$. We will denote as $X_G(\ell) := G \backslash X(\ell)$ the quotient of the modular curve $X(\ell)$ by the action of G on the full level ℓ -structure. The modular curve $X_G(\ell)$ has a geometrically irreducible model over $\mathbb{Q}(\zeta_\ell)^{\det(G)}$, see [12, pp. 115 – 116] or [4, IV, 3.20.4].

In particular, if G is the Borel subgroup we will define, as usual, the modular curve $X_0(\ell) := X_G(\ell)$ over \mathbb{Q} . This modular curve parametrizes elliptic curves with a cyclic ℓ -isogeny, that is, pairs (E, C) , where E is a generalized elliptic curve and C is the kernel of a cyclic ℓ -isogeny, up to isomorphism.

If G is a split Cartan subgroup (respectively, the normalizer of a split Cartan subgroup) we will denote the modular curve $X_G(\ell) := X_{\text{sp.Car}}(\ell)$ (respec-

tively, $X_{\text{split}}(\ell)$). The curve $X_{\text{sp.Car}}(\ell)$ (respectively, $X_{\text{split}}(\ell)$) parametrizes elliptic curves endowed with an ordered (respectively, unordered) pair of independent cyclic ℓ -isogenies.

Following [12], we will denote as $X_{A_4}(\ell)$ (respectively $X_{S_4}(\ell)$, $X_{A_5}(\ell)$) the modular curves obtained taking as $G \subset GL_2(\mathbb{Z}/\ell\mathbb{Z})$ the inverse image of $A_4 \subset PGL_2(\mathbb{Z}/\ell\mathbb{Z})$ (respectively $S_4, A_5 \subset PGL_2(\mathbb{Z}/\ell\mathbb{Z})$). Let us remark that exceptional projective images A_4, S_4 and A_5 can occur only for particular values of ℓ , see [15, section 2.5, 2.6]. The modular curves $X_{A_4}(\ell)$ and $X_{A_5}(\ell)$ have geometrically irreducible models over the quadratic subfield of $\mathbb{Q}(\zeta_\ell)$. The same holds for $X_{S_4}(\ell)$ if $\ell \not\equiv \pm 3 \pmod{8}$, otherwise the model is defined over \mathbb{Q} .

Remark 5.1. Let E/K be an elliptic curve which is occurring in an exceptional pair $(\ell, j(E))$ for the number field K . Let us suppose that the projective image of $\rho_{E,\ell}$ is dihedral. Hence, $(E, \rho_{E,\ell})$ corresponds to a K -rational point in $X_{\text{split}}(\ell)$ by Lemma 2.3 and Corollary 3.6. Moreover, $E[\ell](\overline{K})$ contains two conjugate lines L_1 and L_2 over L/K , where L/K is quadratic (Propositions 3.4 and 3.8). These lines correspond to the isogenies $\alpha : E \rightarrow E/L_1$ and $\beta : E \rightarrow E/L_2$ defined over L . Hence, they give a pair of L -rational points (taking respectively $\alpha\beta^\vee$ and $\beta\alpha^\vee$ as isogeny structure) on $X_0(\ell^2)$ which are conjugate by the Fricke involution w_{ℓ^2} , for a definition see [13, section 2]. Let us recall that there exists a isomorphism defined over \mathbb{Q} between $X_0(\ell^2)$ and $X_{\text{sp.Car}}(\ell)$.

Remark 5.2. If $(\ell, j(E))$ is an exceptional pair for the number field K and $\sqrt{(-\frac{1}{\ell})} \ell \notin K$ then the prime ℓ is congruent to 3 mod 4 and hence to 7 or 11 mod 12, while if $\sqrt{(-\frac{1}{\ell})} \ell \in K$ then the prime ℓ is congruent to 1 mod 4 and hence to 1 or 5 mod 12.

5.1 The case $11 \leq \ell \leq \ell_K$

Theorem 5.3. *If $\ell > 7$, then the number of exceptional pairs $(\ell, j(E))$, for a given number field K , is finite.*

Proof. Given an exceptional pair $(\ell, j(E))$ for the number field K it corresponds to a K -rational point on one of the following modular curves: $X_{\text{split}}(\ell)$, $X_{A_4}(\ell)$, $X_{S_4}(\ell)$ or $X_{A_5}(\ell)$, by Lemmas 2.3 and 3.5. Let us analyze each possible case.

Let us recall that the genus of $X_{\text{split}}(\ell)$ is given by the following formula, for a reference [12, pg. 117]:

$$g(X_{\text{split}}(\ell)) = \frac{1}{24} \left(\ell^2 - 8\ell + 11 - 4 \left(\frac{-3}{\ell} \right) \right).$$

Hence, if $\ell \equiv 1$ or $7 \pmod{12}$, then $g(X_{\text{split}}(\ell)) = \frac{1}{24}(\ell^2 - 8\ell + 7)$. Otherwise, if $\ell \equiv 5$ or $11 \pmod{12}$, then $g(X_{\text{split}}(\ell)) = \frac{1}{24}(\ell^2 - 8\ell + 15)$. Therefore, the modular curve $X_{\text{split}}(\ell)$ has genus larger than 2 for $\ell \geq 11$, and has only finitely many K -rational points by Faltings Theorem.

Let us now study the modular curves $X_{A_4}(\ell)$, $X_{S_4}(\ell)$ and $X_{A_5}(\ell)$. The genus of these modular curves is given by the following formulae, see [2, section 2]:

$$\begin{aligned} g(X_{A_4}(\ell)) &= \frac{1}{288}(\ell^3 - 6\ell^2 - 51\ell + 294 + 18\epsilon_2 + 32\epsilon_3) \\ g(X_{S_4}(\ell)) &= \frac{1}{576}(\ell^3 - 6\ell^2 - 87\ell + 582 + 54\epsilon_2 + 32\epsilon_3) \\ g(X_{A_5}(\ell)) &= \frac{1}{1440}(\ell^3 - 6\ell^2 - 171\ell + 1446 + 90\epsilon_2 + 80\epsilon_3) \end{aligned}$$

where ϵ_2 is equal to 1 if $\ell \equiv 1 \pmod{4}$ and to -1 if $\ell \equiv 3 \pmod{4}$, and ϵ_3 is equal to 1 if $\ell \equiv 1 \pmod{3}$ and to -1 if $\ell \equiv -1 \pmod{3}$. We stress again that these exceptional cases occur only for certain values of ℓ , see [15, section 2.5, 2.6], and the formulae given will not be integral for general values of ℓ , as already noticed in [2, p. 3072]. By Corollary 3.7 if an exceptional pair has projective image isomorphic to A_4 then $\ell \equiv 1 \pmod{12}$ and we have that the genus of $X_{A_4}(\ell)$ is greater than 2 for all $\ell \geq 13$. Similarly for projective image isomorphic to S_4 or to A_5 the genus of the respective modular curves is larger than 2 for primes satisfying the appropriate congruence. \square

5.2 The case $\ell = 5$

Now we will study the local-global principle for 5-isogenies. In order to do so it will be relevant to recall the structure of $X(5)$ at the cusps. The modular interpretation of $X(5)(\overline{\mathbb{Q}})$ associates with each cusp a Néron polygon \mathcal{P} with 5 sides. The Néron polygon is endowed with the structure of generalized elliptic curve and enhanced with a basis of $\mathcal{P}[5] \cong \mu_5 \times \mathbb{Z}/5\mathbb{Z}$, where μ_5 is the set of 5-th root of unity, up to automorphisms of \mathcal{P} :

$$\begin{aligned} (\{\pm 1\} \times \mu_5) \times \mathcal{P}[5] &\rightarrow \mathcal{P}[5] \\ \left(\begin{pmatrix} \epsilon & \alpha \\ 0 & \epsilon \end{pmatrix}, \begin{pmatrix} w \\ j \end{pmatrix} \right) &\mapsto \begin{pmatrix} w^\epsilon \alpha^j \\ \epsilon j \end{pmatrix} \end{aligned}$$

where $\epsilon \in \{\pm 1\}$ and $\alpha, w \in \mu_n$. The set of cusps of $X(5)(\overline{\mathbb{Q}})$ is a Galois set with an action of $GL_2(\mathbb{Z}/5\mathbb{Z})$. The modular interpretation of $X_G(5)$ associates to each cusp an orbit of the enhanced Néron polygon under the action of the group generated by G .

The local-global principle for 5-isogenies is related with V_4 , the Klein 4-group. Let us recall that there is a unique non-trivial 2-dimensional irreducible projective representation τ of V_4 in $\text{PGL}_2(\mathbb{F}_5)$ and, up to conjugation,

tion, this representation is given by:

$$\left\{ \overline{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}, \overline{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}, \overline{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}, \overline{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}} \right\}.$$

For a prime $\ell \geq 5$, we will denote as $X_{V_4}(\ell)$ the modular curves $X_G(\ell)$ obtained taking as $G \subset GL_2(\mathbb{Z}/\ell\mathbb{Z})$ the inverse image of $V_4 \subset PGL_2(\mathbb{Z}/\ell\mathbb{Z})$.

Proposition 5.4. *Over $\text{Spec}(\mathbb{Q}(\sqrt{5}))$ the modular curve $X_{V_4}(5)$ is isomorphic to \mathbb{P}^1 .*

Proof. The genus of $X(5)$ over $\mathbb{Q}(\zeta_5)$ is 0. The field of constants of $X_{V_4}(5)$ is $\mathbb{Q}(\zeta_5)^{\det(G)}$ where G is the inverse image of V_4 in $GL_2(\mathbb{F}_5)$. We have $V_4 \subset SL_2(\mathbb{F}_5)/\{\pm 1\}$ and $\mathbb{F}_5^* \subset G$, hence $\det(G) = (\mathbb{F}_5^*)^2$. This means that $X_{V_4}(5)$ is geometrically irreducible over $\mathbb{Q}(\sqrt{5})$ and its genus is 0.

The set of cusps of $X(5)(\overline{\mathbb{Q}})$ is in 1–1 correspondence with the quotient of the group of isomorphisms as \mathbb{F}_5 -vector spaces between \mathbb{F}_5^2 and $\mu_5 \times \mathbb{F}_5$ by the action of $\{\pm 1\} \times \mu_5$. To show that over $\text{Spec}(\mathbb{Q}(\sqrt{5}))$ the modular curve $X_{V_4}(5)$ is isomorphic to \mathbb{P}^1 it is enough to show that the set of $\mathbb{Q}(\sqrt{5})$ -rational points of $X_{V_4}(5)$ is non-empty.

Let $\phi_{\zeta_5} : \mathbb{F}_5^2 \xrightarrow{\sim} \mu_5 \times \mathbb{F}_5$ be the isomorphism given by $\phi_{\zeta_5}((1, 0)) = (\zeta_5, 0)$, $\phi_{\zeta_5}((0, 1)) = (1, 1)$. The orbit of the cusp corresponding to ϕ_{ζ_5} under the action of $\{\pm 1\} \times \mu_5$ is the following set:

$$\begin{aligned} & \{((\zeta_5, 0), (1, 1)), ((\zeta_5^{-1}, 0), (1, -1)), ((\zeta_5, 0), (\zeta_5, 1)), ((\zeta_5^{-1}, 0), (\zeta_5^{-1}, -1)), \\ & ((\zeta_5, 0), (\zeta_5^2, 1)), ((\zeta_5^{-1}, 0), (\zeta_5^{-2}, -1)), ((\zeta_5, 0), (\zeta_5^{-2}, 1)), \\ & ((\zeta_5^{-1}, 0), (\zeta_5^2, -1)), ((\zeta_5, 0), (\zeta_5^{-1}, 1)), ((\zeta_5^{-1}, 0), (\zeta_5, -1))\}. \end{aligned}$$

On the set of cusps we have a Galois action by $\text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$. In particular, acting with $-1 \in \text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ on the cusp $((\zeta_5, 0), (1, 1))$ we obtain the cusp $((\zeta_5^{-1}, 0), (1, 1))$ which does not define the same cusps on $X(5)(\overline{\mathbb{Q}})$.

However, the action of $-1 \in \text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ on the class of the cusp $((\zeta_5, 0), (1, 1))$ preserve the orbit of the cusp under G : in fact G , inverse image of V_4 in $GL_2(\mathbb{F}_5)$, is the group given by $\left\{ \begin{pmatrix} x & 0 \\ 0 & \pm x \end{pmatrix}, \begin{pmatrix} 0 & \pm x \\ x & 0 \end{pmatrix} \mid x \in \mathbb{F}_5^* \right\}$,

and under the action of $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in G$ the cusp $((\zeta_5^{-1}, 0), (1, 1))$ of $X(5)(\overline{\mathbb{Q}})$ is mapped to $((\zeta_5, 0), (1, 1))$.

It follows that the cusp $((\zeta_5, 0), (1, 1))$ in $X_{V_4}(5)(\overline{\mathbb{Q}})$ is stable under $\text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5}))$. This implies that $X_{V_4}(5)(\mathbb{Q}(\sqrt{5}))$ is non-empty. \square

Corollary 5.5. *There exist infinitely many exceptional pairs $(5, j(E))$ for the number field K if and only if $\sqrt{5}$ belongs to K .*

Proof. By Proposition 3.9, there is an exceptional pair $(5, j(E))$ for the number field K only if $\sqrt{5}$ belongs to K . If $(5, j(E))$ is an exceptional pair for the number field K then the projective image of the Galois representation associated to the elliptic curve E over K is a dihedral group of order dividing 8 (Lemma 3.5 combined with Corollary 3.7). In particular, the image projective image of the Galois representation can be the Klein 4-group V_4 . Since by Proposition 5.4 over $\text{Spec}(\mathbb{Q}(\sqrt{5}))$ the modular curve $X_{V_4}(5)$ is isomorphic to \mathbb{P}^1 , then $X_{V_4}(5)(K)$ is non-empty if and only if $\sqrt{5}$ belongs to K . In particular, if $\sqrt{5}$ belongs to K then there exist infinitely many exceptional pairs $(5, j(E))$ since $X_{V_4}(5)$ is isomorphic to \mathbb{P}^1 over $\text{Spec}(K)$. \square

5.3 The case $\ell = 7$

The local-global principle for 7-isogenies leads us to a dichotomy between a finite and an infinite number of counterexamples according to the rank of a specific elliptic curve that we call the Elkies-Sutherland curve:

Proposition 5.6. *If $\ell = 7$ then the number of exceptional pairs $(7, j(E))$ for a number field K , is finite or infinite, depending on the rank of the elliptic curve*

$$E' : y^2 = x^3 - 1715x + 33614$$

being 0 or positive respectively.

Proof. If $\sqrt{-7} \in K$ then by Lemma 3.5 there is no exceptional pair. Let us suppose that $\sqrt{-7}$ is not in K . As shown by Sutherland in [17, section 3] and explained in Remark 5.1, the modular curve to deal with is the twist of $X_0(49)$ by $\text{Gal}(K(\sqrt{-7})/K)$ with respect to w_{49} , the Fricke involution on $X_0(49)$. Using the computations done by Elkies, as stated in [17, section 3], we have that each $K(\sqrt{-7})$ -rational point of E' corresponds to a class of isomorphism of elliptic curves over K , such that every elliptic curve in the class gives an exceptional pair at 7. Explicitly, if the $K(\sqrt{-7})$ -rational point of E' has coordinates (u, v) , let $t = (3u - v + 42)/(u + 2v)$, then the j -invariant of the isomorphism class of elliptic curves which are exceptional for the local-global principle for 7-isogenies is equal to

$$\frac{-(t-3)^3(t-2)(t^2+t-5)^3(t^2+t+2)^3(t^4-3t^3+2t^2+3t+1)^3}{(t^3-2t^2-t+1)^7}.$$

Hence, if the rank of E' over K is positive there are infinitely many counterexamples to the local-global principle about 7-isogenies, while if the rank is 0 there are only finitely many. \square

Remark 5.7. As shown by Sutherland in [17, section 3], over $\mathbb{Q}(i)$ the curve E has positive rank, so there are infinitely many counterexamples on this field to the local-global principle about 7-isogenies.

The proof of our Main Theorem (see Introduction) is now complete.

5.4 Examples for the case $\ell = 7$.

Let E be an elliptic curve defined over a number field K . The global L -series $L_E(s, K)$ of E , see [16, p. 449], is formally defined by the Euler product:

$$L_E(s, K) = \prod_{\substack{v \\ \text{good reduction}}} (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1} \cdot \prod_{\substack{v \\ \text{bad reduction}}} (1 - a_v q_v^{-s})^{-1}$$

where q_v is the cardinality of the residue field k_v of K at v and if E has bad reduction at v then $a_v = 0, 1$ or -1 according to the reduction type, while if E has good reduction at v then a_v satisfies $|\overline{E}(k_v)| = q_v + 1 - a_v$.

Once defined the L -function attached to an elliptic curve over a number field, we can state the following conjectures:

Conjectures. *Let E/K be an elliptic curve over a number field K .*

- **Hasse-Weil Conjecture.** *The L -function $L_E(s, K)$ has an analytic continuation to \mathbb{C} and satisfies a functional equation*

$$L_E^*(s, K) = w(E/K) L_E^*(2 - s, K),$$

where $w(E/K)$ is called root number and determines the sign of the functional equation.

- **Birch-Swinnerton-Dyer Conjecture.** *The L -function $L_E(s, K)$ satisfies: $\text{ord}_{s=1} L_E(s, K) = r$, where r is the rank of $E(K)$.*
- **Parity Conjecture:** $(-1)^r = w(E/K)$.

Let E be the elliptic curve $y^2 = x^3 - 1715x + 33614$ over a number field K , not containing $\sqrt{-7}$. If we assume that the parity conjecture holds true, then if the rank of the L -function $L_E(s, K)$ is odd, there are infinitely many counterexamples to the local-global principle about 7-isogenies.

For $\mathbb{Q}(\sqrt{-23})$, by an easy computation in SAGE, it is possible to show that $L_E(s, \mathbb{Q}(\sqrt{-23}))$ has odd analytic rank, hence the curve E has positive rank, so there are infinitely many counterexamples on this field to the local-global principle about 7-isogenies. Note that, since this is a degree 2 extension of \mathbb{Q} , according to Theorem 4.3, the only primes for which the local-global principle could fail are 7, 11 and 23. For 11 and 23 there are only finitely many counterexamples by our Main Theorem.

On the other hand, using SAGE, we have been able to show that the rank of the elliptic curve $y^2 = x^3 - 1715x + 33614$ is zero on the number fields $\mathbb{Q}(\sqrt{-D})$ for D in the following list:

$$D = 14, 21, 35, 42, 91, 105, 119, 133, 154, 161, 182, 203, 217, 231, 238, 259, 287.$$

We have obtained this list using the fact that the L -function of E over a quadratic extension of the rational by \sqrt{d} , for an integer d , is equal to the product of the L -function of E over \mathbb{Q} times the L -function of the d -quadratic twist of E over \mathbb{Q} .

6 Complex multiplication

Sutherland in [17] proved that an exceptional pair $(\ell, j(E))$ over \mathbb{Q} cannot have complex multiplication: for $\ell > 7$ we refer to the proof of [17, Theorem 2] and for $\ell = 7$ we refer to the direct computations in [17, section 3]. Here we study the same problem for K a number field.

Lemma 6.1. *Let K be a number field and E/K an elliptic curve over K , $j(E) \notin \{0, 1728\}$. Let $(\ell, j(E))$ be an exceptional pair for K . If $\ell > 2d+1$ then E cannot have complex multiplication.*

Proof. Assume that E has complex multiplication by a quadratic order \mathcal{O} . This means that the Galois representation $\rho_{E, \ell}$ has image included in a Borel, when ℓ ramifies in \mathcal{O} , or projectively dihedral (split or nonsplit, according to ℓ being split or nonsplit in \mathcal{O}), see [14, Théorème 5]. The Borel case is clearly not possible. By Proposition 3.4, there is an ℓ -isogenous elliptic curve E' that is defined over a quadratic extension L of K , but not over K , since we are in an exceptional case. Since E' is isogenous to E over L , it also must have complex multiplication by an order \mathcal{O}' . Since E and E' are ℓ -isogenous, by [3, Theorem 7.24], the ratio between the class numbers $h(\mathcal{O}')$ and $h(\mathcal{O})$ satisfies

$$\frac{h(\mathcal{O}')}{h(\mathcal{O})} = \frac{1}{[\mathcal{O}^* : \mathcal{O}'^*]} \left(\ell - \left(\frac{\text{disc}(\mathcal{O})}{\ell} \right) \right) \geq (\ell-1)$$

since $j(E) \notin \{0, 1728\}$. In particular if $h(\mathcal{O}') = h(\mathcal{O})$ we have a contradiction. Hence assume $h(\mathcal{O}') > h(\mathcal{O})$. Since E' is defined over L and E is defined over K then we know that $\mathbb{Q}(j_E) \subseteq K$ and $\mathbb{Q}(j_{E'}) \subseteq L$. Then the ratio of the class numbers $h(\mathcal{O}')$ and $h(\mathcal{O})$ satisfies:

$$\frac{h(\mathcal{O}')}{h(\mathcal{O})} \leq [L : \mathbb{Q}] = 2d.$$

Hence, if $\ell > 2d + 1$, we have a contradiction between the lower and the upper bound, so E cannot have complex multiplication. \square

Acknowledgements

I would like to thank my advisor, Pierre Parent, for his advices, his guidance and patience throughout the many readings and corrections of this article. I also am very grateful to my advisor, Bas Edixhoven, for all the fruitful discussions about this topic.

References

- [1] B. J. BIRCH AND W. KUYK, *Modular functions of one variable. IV*, Lecture Notes in Mathematics, Vol. 476, Springer-Verlag, Berlin, 1975.
- [2] A. C. COJOCARU AND C. HALL, *Uniform results for Serre's theorem for elliptic curves*, International Mathematics Research Notices, (2005), pp. 3065–3080.
- [3] D. A. COX, *Primes of the form $x^2 + ny^2$* , A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.
- [4] P. DELIGNE AND M. RAPOPORT, *Les schémas de modules de courbes elliptiques*, in Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.
- [5] L. E. DICKSON, *Linear groups: With an exposition of the Galois field theory*, with an introduction by W. Magnus, Dover Publications Inc., New York, 1958.
- [6] B. H. GROSS, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. J., 61 (1990), pp. 445–517.
- [7] N. M. KATZ, *Galois properties of torsion points on abelian varieties*, Inventiones mathematicae, 62 (1981), pp. 481–502.
- [8] N. M. KATZ AND B. MAZUR, *Arithmetic moduli of elliptic curves*, vol. 108 of Annals of Mathematics Studies, Princeton University Press, Princeton, NJ, 1985.
- [9] A. KRAUS, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math., 69 (1990), pp. 353–385.
- [10] S. LANG, *Introduction to modular forms*, Springer-Verlag, Berlin, 1976.
- [11] B. MAZUR, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math., (1977), pp. 33–186 (1978).
- [12] ———, *Rational points on modular curves*, in Modular Functions of one Variable V, J.-P. Serre and D. Zagier, eds., vol. 601 of Lecture Notes in Mathematics, Springer Berlin Heidelberg, 1977, pp. 107–148.
- [13] P. J. R. PARENT, *Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$* , Compos. Math., 141 (2005), pp. 561–572.
- [14] J.-P. SERRE, *Groupes de Lie l -adiques attachés aux courbes elliptiques*, in Les Tendances Géom. en Algèbre et Théorie des Nombres, Éditions du Centre National de la Recherche Scientifique, Paris, 1966, pp. 239–256.
- [15] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones mathematicae, 15 (1972), pp. 259–331.
- [16] J. H. SILVERMAN, *The arithmetic of elliptic curves*, vol. 106 of Graduate Texts in Mathematics, Springer, Dordrecht, second ed., 2009.
- [17] A. V. SUTHERLAND, *A local-global principle for rational isogenies of prime degree*, J. Théor. Nombres Bordeaux, 24 (2012), pp. 475–485.

MI, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands	IMB, Université Bordeaux 1, 351, cours de la Libération, F 33405 TALENCE cedex France
---	--

E-mail address: sannni@math.leidenuniv.nl